Blockchain Security Monthly Recap of August: $17.43M lost in attacks

Beosin · Follow

5 min read · 1 day ago

2

According to Beosin EagleEye, a blockchain security company under Beosin, various types of security incidents and losses in August 2023 have significantly decreased compared to July. In August, there were over 25 typical security incidents, with a total loss of approximately $17.43 million, a decrease of about 90% compared to July. The total amount involved in Rug Pull incidents reached $28.85 million, an increase of about 18% compared to July.

The largest attack incident this month occurred on the Optimism's Exactly Protocol, resulting in a loss of approximately $7.3 million. There has been an increase in exit scam incidents this month, with notable cases including a $15.5 million outflow from the PEPE multisig wallet, attributed to "three former team members" according to the official statement. Additionally, the Magnate Finance project on the Base chain experienced a Rug Pull, resulting in a loss of about $6.5 million. Furthermore, there has been an increase in law enforcement cracking down on cryptocurrency-related criminal cases this month, involving several cases worth over a hundred million dollars. The largest case was a $1 billion money laundering case cracked by the Singapore police.

DeFi

『9』Typical Incidents

№1 — On August 2nd, Uwerx Network was attacked, resulting in a loss of approximately $320,000.

№2 — On August 8th, the stablecoin protocol Steadifi was attacked, with the attacker gaining control of the wallet of the protocol deployer, resulting in a loss of about $1.14 million.

№3 — On August 9th, the DeFi project Earning Farm was hit by a reentrancy attack, causing a loss of approximately $530,000.

№4 — On August 14th, the DeFi yield aggregation protocol Zunami Protocol was manipulated through price manipulation, resulting in a loss of about $2.1 million.

№5 — On August 15th, RocketSwap on the Base chain was attacked due to private key compromise, with the hacker profiting around $870,000.

№6 — On August 18th, the DeFi lending protocol Exactly Protocol was attacked, leading to a loss of approximately $7.3 million.

№7 — On August 19th, the Cosmos ecosystem cross-chain stablecoin protocol Harbor Protocol was attacked, causing a loss of about $18,000.

№8 — On August 20th, the derivative market Thales was attacked due to private key compromise, resulting in a loss of about $13,000 on the BNB Chain.

№9 — On August 26th, the STV token on the BNB Chain was attacked, causing a loss of approximately $400,000.

DEX

『3』Typical Incidents

№1 — On August 1st, the decentralized exchange LeetSwap on the BASE chain experienced a price manipulation attack, resulting in a loss of approximately $620,000.

№2 — On August 7th, the Solana-based decentralized exchange Cypher was attacked, causing a loss of about $1 million.

№3 — On August 23rd, Balancer reported a serious vulnerability affecting multiple V2 pools. The vulnerability had not been exploited yet, and users were advised to withdraw their funds. On August 27th, Balancer was subjected to multiple flash loan attacks by hackers. The hackers profited a total of about $2.1 million from both the Balancer and Beethoven X projects.

Rug Pull

『6』Typical Incidents

№1 — On August 3rd, a Rug Pull occurred on the BNB Chain's Apache NFT SalesRoom (ASN), with the deployer profiting approximately $680,000.

№2 — On August 6th, the Bitlord project executed a Rug Pull, resulting in the deployer gaining around $560,000.

№3 — On August 16th, the SwirlLend project on the Base chain conducted a Rug Pull, leading to the deployer making over $500,000 in profit.

№4 — On August 21st, a fraudulent "LayerZero" token executed a Rug Pull on the BNB Chain, resulting in the deployer profiting $1 million.

№5 — On August 24th, the PEPE multisig wallet adjusted its threshold from 5/8 to 2/8. More than 160 trillion PEPE tokens (equivalent to about $15.5 million) were transferred from the PEPE multisig wallet to platforms like Binance, OKX, and Bybit. On August 26th, the PEPE official statement revealed that internal conflicts had been troubling the project since its inception, and the token sale was attributed to actions taken by three former team members.

№6 — On August 25th, on the Base chain, Magnate Finance executed a Rug Pull by directly manipulating the price oracle, resulting in a loss of approximately $6.5 million. The deployer's address is linked to previous scams involving Solfire and Kokomo Finance.

Cryptocurrency Crime/Regulation

『7』Typical Incidents

№1 — On August 8th, it was reported that law enforcement authorities in the Indian state of Odisha successfully dismantled a cryptocurrency Ponzi scheme valued at $120 million (10 billion INR). The project involved was named The Solar Techno Alliance (STA).

№2 — On August 9th, authorities in Hubei, China, cracked down on a virtual currency money laundering case, with a total laundered amount reaching RMB 300 million.

№3 — On August 16th, according to official sources from the Singapore Police Force, the Singaporean police arrested 10 foreign suspects for money laundering and document forgery. The total value of the involved assets amounted to around 1 billion Singapore Dollars (approximately $740 million), making it the largest money laundering case in Singapore's history.

№4 — On August 23rd, Israeli authorities, after a two-year investigation, charged businessman Moshe Hogeg and his partners with defrauding investors of a value of $290 million in cryptocurrency.

№5 — On August 24th, according to an official announcement, the U.S. Department of Justice charged Tornado Cash founders Roman Storm and Roman Semenov with conspiring to launder money, violating sanctions, and operating an unlicensed money transmitting business.

№6 — On August 27th, Hong Kong police launched an anti-money laundering operation this month, arresting 458 individuals suspected of money laundering and related offenses, involving an amount of HK$470 million.

№7 — On August 30th, Shanxi police dismantled a criminal gang involved in "money laundering" through the sale of gold and virtual currency, with the total involved amount reaching RMB 135 million.

Given the current new developments in the blockchain security landscape, here are Beosin's recommendations:

Overall, in August 2023, various types of blockchain security incidents and the associated losses have significantly decreased. The total amount lost due to hacker attacks in August was approximately $17.43 million, marking a reduction of about 90% compared to July. There has been an increase in attacks and exit scam incidents on the Base chain. Users are advised to conduct thorough research before participating in Base projects to mitigate the risk of financial losses.

This month, 60% of attacks still originated from exploiting contract vulnerabilities. Therefore, it is strongly recommended that project teams seek out professional security companies to conduct audits before launching their projects. This proactive measure can help identify and rectify potential vulnerabilities, safeguarding both user funds and the project's reputation.

Contact

If you need any blockchain security services, welcome to contact us:

Official Website Twitter Telegram Linkedin